(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
30 juin 2005 (30.06.2005)

PCT

(10) Numéro de publication internationale
WO 2005/060205 A1

(51) Classification internationale des brevets[7] :
H04L 29/06, G06F 17/30

(21) Numéro de la demande internationale :
PCT/FR2004/003252

(22) Date de dépôt international :
16 décembre 2004 (16.12.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0314833 17 décembre 2003 (17.12.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **MORIN, Benjamin** [FR/FR]; 22, rue des Croisières, F-14000 Caen (FR). **DEBAR, Hervé** [FR/FR]; 7, rue des Semailles, F-14111 Louvigny (FR).

(74) Mandataires : **JOLY, Jean-Jacques** etc.; Cabinet Beau de Loménie, 158, rue de l'Université, F-75340 Paris Cedex 07 (FR).

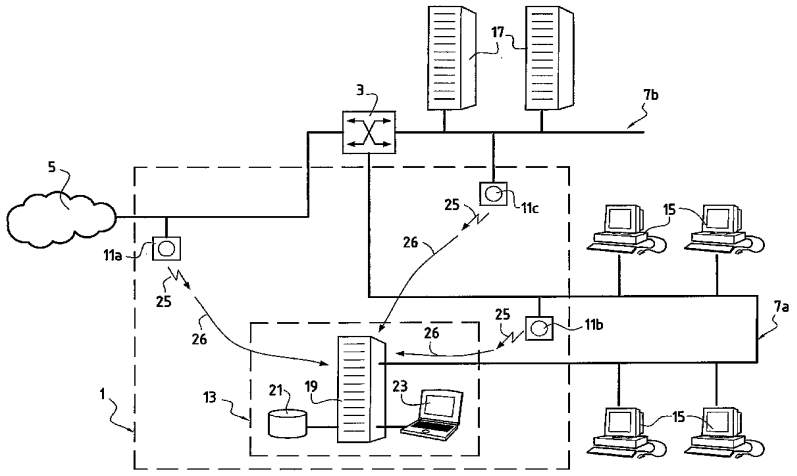
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH,

[Suite sur la page suivante]

(54) **Title:** METHOD FOR MANAGING A SET OF ALARMS EMITTED BY SENSORS FOR DETECTING INTRUSIONS OF A INFORMATION SECURITY SYSTEM

(54) **Titre :** PROCEDE DE GESTION D'UN ENSEMBLE D'ALERTES ISSUES DE SONDES DE DETECTION D'INTRUSIONS D'UN SYSTEME DE SECURITE D'INFORMATIONS.



(57) **Abstract:** The invention relates to a method for managing a set of alarms emitted by intrusion detecting sensors (11a, 11b, 11c) of an information security system (1) comprising an alarm managing system (13), wherein each alarm is identified by an alarm identifier and an alarm content consisting in assigning a description comprising a conjunction of a plurality of valued attributes allocated to a plurality of attribute ranges to each alarm emitted by said intrusion detecting sensors (11a, 11b, 11c), organising the valued attributes allocated to each attribute range into a taxonomic structure defining generalisation ratios between said valued attributes and the plurality of attribute ranges forming the structure of taxonomic structures, completing the description of each said alarm by a set of values induced by the taxonomic structures from the valued attribute of said alarms in order to form completed alarms and in storing said completed alarms in a logic files (21) in such a way that it is possible to reference thereon.

[Suite sur la page suivante]

WO 2005/060205 A1

GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions (11a, 11b, 11c) d'un système de sécurité d'informations (1) comportant un système de gestion d'alertes (13), chaque alerte étant définie par un identifiant d'alerte et un contenu d'alerte, le procédé comportant les étapes suivantes -associer à chacune des alertes issues des sondes de détection d'intrusions (11a, 11b, 11c), une description comportant une conjonction d'une pluralité d'attributs valués appartenant à une pluralité de domaines d'attributs ; -organiser les attributs valués appartenant à chaque domaine d'attributs en une structure taxinomique définissant des relations de généralisation entre lesdits attributs valués, la pluralité des domaines d'attributs formant ainsi une pluralité de structures taxinomiques ; -compléter la description de chacune desdites alertes par des ensembles de valeurs induites par les structures taxinomiques à partir des attributs valués desdites alertes pour former des alertes complètes ; -stocker lesdites alertes complètes dans un système de fichiers logique (21) pour en permettre la consultation.

Titre de l'invention

Procédé de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions d'un système de sécurité d'informations.

Arrière-plan de l'invention

L'invention concerne un procédé de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions.

La sécurité des systèmes d'information passe par le déploiement de systèmes de détection d'intrusions « IDS » comportant des sondes de détection d'intrusions qui émettent des alertes vers des systèmes de gestion d'alertes.

En effet, les sondes de détection d'intrusions sont des composants actifs du système de détection d'intrusions qui analysent une ou plusieurs sources de données à la recherche d'événements caractéristiques d'une activité intrusive et émettent des alertes vers les systèmes de gestion d'alertes. Un système de gestion des alertes centralise les alertes provenant des sondes et effectue éventuellement une analyse de l'ensemble de ces alertes.

Les sondes de détection d'intrusions génèrent un très grand nombre d'alertes qui peut comprendre plusieurs milliers par jour en fonction des configurations et de l'environnement.

L'excès d'alertes peut résulter d'une combinaison de plusieurs phénomènes. Tout d'abord, de fausses alertes représentent jusqu'à 90% du nombre total d'alertes. Ensuite, les alertes sont souvent trop granulaires, c'est-à-dire que leur contenu sémantique est très pauvre. Enfin les alertes sont souvent redondantes et récurrentes.

Ainsi, l'excès d'alertes rend leur compréhension et leur manipulation difficile par un opérateur de sécurité humain.

Le traitement amont des alertes au niveau du système de gestion est donc nécessaire pour faciliter le travail d'analyse de l'opérateur de sécurité.

Les systèmes de gestion d'alertes actuels consistent à stocker les alertes dans un système de gestion de bases de données relationnelles (SGBDR). L'opérateur de sécurité peut ainsi interroger ce système de gestion SGBDR en lui soumettant une requête portant sur les propriétés des alertes. Le système de gestion SGBDR fournit en retour à l'opérateur, l'ensemble des alertes dont la description satisfait la requête.

L'inconvénient de ces systèmes est le fait que les alertes fournies à l'opérateur peuvent être nombreuses et granulaires, ce qui rend leur analyse fastidieuse.

Objet et résumé de l'invention

L'invention a pour but de remédier à ces inconvénients, et de fournir une méthode simple de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions pour permettre une consultation flexible, aisée et rapide de cet ensemble d'alertes.

Ces buts sont atteints grâce à un procédé de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions d'un système de sécurité d'informations comportant un système de gestion d'alertes, chaque alerte étant définie par un identifiant d'alerte et un contenu d'alerte, caractérisé en ce qu'il comporte les étapes suivantes :

-associer à chacune des alertes issues des sondes de détection d'intrusions, une description comportant une conjonction d'une pluralité d'attributs valués appartenant à une pluralité de domaines d'attributs ;

-organiser les attributs valués appartenant à chaque domaine d'attribut en une structure taxinomique définissant des relations de généralisation entre lesdits attributs valués, la pluralité des domaines d'attributs formant ainsi une pluralité de structures taxinomiques ;

-compléter la description de chacune desdites alertes par des ensembles de valeurs induites par les structures taxinomiques à partir des attributs valués desdites alertes pour former des alertes complètes ;

-stocker lesdites alertes complètes dans un système de fichiers logique pour en permettre la consultation.

Ainsi, le stockage des alertes complètes dans un système de fichiers logique permet à un opérateur de sécurité de consulter le système de gestion d'alertes d'une manière efficace, rapide, et flexible afin d'obtenir une vision précise de l'ensemble des alertes issues des sondes de détection d'intrusions.

La consultation des alertes complètes peut être réalisée par une succession d'interrogations et/ou de navigations dans lesdites alertes complètes de sorte qu'en réponse à une requête, le système de gestion d'alertes fournit des attributs valués pertinents permettant de distinguer un sous-ensemble d'alertes complètes parmi un ensemble d'alertes complètes satisfaisant la requête afin de permettre le raffinement de ladite requête.

De préférence, les attributs valués pertinents sont en priorité les plus généraux en regard de la pluralité des structures taxinomiques.

Avantageusement, en réponse à la requête, le système de gestion d'alertes fournit en outre des identifiants d'alertes satisfaisant la requête et dont la description ne peut pas être raffinée par rapport à ladite requête.

L'identifiant d'alerte est un couple formé d'un identifiant de la sonde de détection d'intrusions qui produit l'alerte et d'un numéro de série d'alerte affecté par ladite sonde.

Le contenu de chaque alerte comporte un message textuel fourni par la sonde de détection d'intrusions correspondante.

Chaque attribut valué comporte un identifiant d'attribut et une valeur d'attribut.

Selon un aspect de l'invention, chaque identifiant d'attribut est associé à un domaine d'attributs parmi les domaines suivants : domaine de l'attaque, domaine de l'identité de l'attaquant, domaine de l'identité de la victime et domaine de la date de l'attaque.

Avantageusement, la description d'une alerte donnée est complétée en récupérant à partir des relations de généralisation de la pluralité de structures taxinomiques et de manière récursive, un ensemble comportant les attributs valués plus généraux et n'ayant pas déjà été présents dans la description d'une autre alerte précédemment complétée.

Selon un aspect particulier de l'invention, les attributs valués dans la structure taxinomique sont organisés selon un graphe acyclique dirigé.

L'invention vise aussi un programme informatique conçu pour mettre en œuvre le procédé ci-dessus, lorsqu'il est exécuté par le système de gestion d'alertes.

Brève description des dessins

D'autres particularités et avantages de l'invention ressortiront à la lecture de la description faite, ci-après, à titre indicatif mais non limitatif, en référence aux dessins annexés, sur lesquels :

-la figure 1 est une vue très schématique d'un système de sécurité d'informations comportant un système de gestion d'alertes selon l'invention ;

-la figure 2 est un organigramme illustrant les étapes du procédé de gestion d'un ensemble d'alertes, selon l'invention ;

-la figure 3A illustre un exemple d'une documentation associée à des signatures d'attaques ; et

-la figure 3B montre de façon très schématique une structure taxinomique associée à l'exemple de la figure 3A.

Description détaillée de modes de réalisation

La figure 1 illustre un exemple d'un système de détection d'intrusions 1 relié à travers un routeur 3 à un réseau externe 5 et à un réseau interne 7a et 7b à architecture distribuée.

Le système de détection d'intrusions 1 comporte plusieurs sondes de détection d'intrusions 11a, 11b, 11c, et un système de gestion d'alertes 13. Ainsi, une première sonde 11a de détection d'intrusions surveille les alertes venant de l'extérieur, une deuxième sonde 11b surveille une partie du réseau interne 7a comprenant des stations de travail 15 et une troisième sonde 11c surveille une autre partie du réseau interne 7b comprenant des serveurs 17 délivrant des informations au réseau externe 5.

Le système de gestion d'alertes 13 comporte un hôte 19 dédié au traitement des alertes, un système de fichiers logique 21, et une unité de sortie 23.

Le système de fichiers logique peut être du type « LISFS » proposé par Padioleau et Ridoux, dans une conférence (Usenix Annual Technical Conference 2003) intitulée "A Logic File System".

Dans le système de fichiers logique LISFS, les fichiers sont des objets auxquels sont associées des descriptions, exprimées dans une logique propositionnelle. La description d'un fichier est une conjonction de propriétés.

Les propriétés des fichiers sont les répertoires du système de fichiers, si bien que le chemin d'un fichier est sa description. Un chemin est donc une formule logique. Un emplacement du système de fichiers contient l'ensemble des fichiers dont la description satisfait la formule correspondant au chemin de l'emplacement.

Comme dans un système de fichiers classique, des commandes spécifiques permettent de naviguer et manipuler les fichiers et leurs descriptions.

Ainsi, les sondes 11a, 11b, 11c déployées dans le système de détection d'intrusions 1 envoient (flèches 26) leurs alertes 25 au système

de gestion d'alertes 13. Ce dernier, conformément à l'invention, procède à une gestion de cet ensemble d'alertes et à son stockage dans le système de fichiers logique 21 pour en permettre la consultation à travers l'unité de sortie 23 d'une manière flexible.

En effet, l'hôte 19 du système de gestion d'alertes 13 comprend des moyens de traitements pour procéder à cette gestion des alertes.

Ainsi, un programme informatique conçu pour mettre en œuvre la présente invention peut être exécuté par le système de gestion d'alertes.

La figure 2 est un organigramme illustrant les étapes du procédé de gestion d'un ensemble $\mathcal{O}$ d'alertes issues de sondes de détection d'intrusions selon l'invention.

Chaque alerte o de cet ensemble $\mathcal{O}$ d'alertes est définie par un identifiant d'alerte et un contenu d'alerte.

En effet, une alerte $o \in \mathcal{O}$ peut être définie par un identifiant d'alertes unique $id(o)$ donné par un couple (s,n) où s est l'identifiant de série de la sonde de détection d'intrusions qui produit l'alerte et n est un numéro de série d'alerte affecté par cette sonde à l'alerte o.

Le contenu m_o de l'alerte o comporte un message textuel fourni par la sonde de détection d'intrusions qui a produit l'alerte et qui est destiné à l'opérateur de sécurité.

L'étape E1 consiste à associer à chacune des alertes issues des sondes de détection d'intrusions 11a, 11b, 11c, une description $d(o)$ comportant une conjonction d'une pluralité d'attributs valués $\{d_{o,i}\}$ appartenant à une pluralité ou un ensemble de domaines d'attributs $\{\mathcal{A}\}$.

Ainsi, une description $d(o)$ d'une alerte est une conjonction de p attributs valués, c'est-à-dire $d(o) = d_{o,1} \wedge \cdots \wedge d_{o,p}$.

Un attribut valué $d_{o,i}$ est un couple (a,v) comportant un identifiant d'attribut a et une valeur d'attribut v.

Chaque identifiant d'attribut a est associé à un domaine d'attribut $\mathcal{A}$ parmi les domaines suivants : domaine de l'attaque, domaine de l'identité de l'attaquant, domaine de l'identité de la victime et domaine de la date de l'attaque.

D'une manière générale, un domaine d'attribut $\mathcal{A}$ est formé d'un ensemble discret muni d'une relation d'ordre partiel $\prec_A$ définissant le domaine de l'attribut valué $d_{o,i}$.

L'étape E2 consiste à organiser les attributs valués $d_{o,i}$ appartenant à chaque domaine d'attribut $\mathcal{A}$ en une structure taxinomique définissant des relations de généralisation (ou spécialisation) entre ces attributs valués. Il existe une taxinomie par domaine d'attribut. Ainsi, la pluralité des domaines d'attributs forme une pluralité de structures taxinomiques.

La structure taxinomique des attributs valués est de manière générique un graphe acyclique dirigé.

Les relations taxinomiques sont modélisées par des axiomes. Ainsi, un attribut valué d plus spécifique qu'un autre attribut valué d' est modélisé par un axiome $d \models d'$, c'est-à-dire que l'attribut valué d' est une conséquence logique de l'attribut valué d. Autrement dit, une alerte qui possède l'attribut valué spécifique d possède automatiquement l'attribut valué moins spécifique d'.

L'étape E3 consiste à compléter la description de chacune des alertes issues des sondes de détection d'intrusions 11a, 11b, 11c, par des ensembles de valeurs induites par les structures taxinomiques, à partir des attributs valués de ces alertes initiales, pour former des alertes complètes.

En effet, les attributs valués des alertes produites par les sondes de détection d'intrusions sont les plus spécifiques des taxinomies.

Ainsi, à la réception d'une alerte donnée, le système de gestion d'alertes 13 peut par exemple compléter la description de cette alerte en récupérant à partir des relations de généralisation de la pluralité de structures taxinomiques et de manière récursive, un ensemble comportant les attributs valués plus généraux et n'ayant pas déjà été présents dans la description d'une autre alerte précédemment complétée.

Autrement dit, la description d'une alerte donnée est complétée par un processus qui consiste à remonter dans une taxinomie donnée à partir d'un attribut valué donné. Si un attribut valué existe déjà dans la description d'une autre alerte précédemment traitée, alors le processus de remontée s'arrête, sinon il est ajouté et le processus est réitéré à partir de cet attribut valué ajouté.

Ci-dessous est un exemple d'un algorithme « *CompléterDescription* » décrivant un processus pour compléter la description d'une alerte.

CompléterDescription
s'il n'existe pas $d_{o,i}$ ***faire***
$D = \{d'_{o,i} : \mathrm{d_{o,i}} \models d'_{o,i}\}$
pour chaque $d'_{o,i} \in D$ ***faire***
CompléterDescription($d'_{o,i}$)
fait
mkdir $d'_{o,1} / \cdots / d'_{o,n}$
fait

Cet algorithme teste tout d'abord l'existence d'un attribut valué donné $d_{o,i}$. Si cet attribut $d_{o,i}$ n'existe pas, on récupère l'ensemble $D = \{d'_{o,i} : \mathrm{d_{o,i}} \models d'_{o,i}\}$ des attributs valués qui sont plus abstraits au regard des taxinomies. Ensuite pour chaque élément $d'_{o,i}$ appartenant à D, l'algorithme *CompléterDescription* est appelé récursivement. A la fin, l'attribut valué est ajouté au système de gestion d'alertes par la

commande « *mkdir* » qui fait partie des commandes du système de fichiers logique LISFS.

Finalement l'étape E4 de la figure 2, consiste à stocker les alertes, qui ont été complétées à l'étape précédente, dans le système de fichiers logique 21 pour en permettre la consultation.

Ci-dessous est un exemple d'un algorithme « *StockerAlerte* » décrivant un processus pour stocker une nouvelle alerte dans un système de fichiers logique du type LISFS.

StockerAlerte
Pour chaque $d_{o,i}$ ***faire***
CompléterDescription($d_{o,i}$)
fait
cp m_o $d_{o,1}/\cdots/d_{o,n}/a$

Cet algorithme complète de manière itérative pour chaque élément de description $d_{o,i}$, une alerte donnée o en appelant l'algorithme « *CompléterDescription* » décrit ci-dessus.

Lorsque tous les éléments de description de l'alerte donnée sont complétés, alors l'alerte complète et son contenu sont stockés par une commande de stockage « *cp* », qui prend en paramètre le contenu de l'alerte m_o, la description de l'alerte $d_{o,1}/\cdots/d_{o,n}$ et l'identifiant de l'alerte a.

Le stockage des alertes complètes dans le système de fichiers logique 21 permet leur consultation par une succession d'interrogations et/ou de navigations dans l'ensemble des alertes complètes.

Ainsi, en réponse à une requête d'un opérateur de sécurité, le système de gestion d'alertes 13 fournit des attributs valués pertinents permettant de distinguer un sous-ensemble d'alertes complètes parmi un ensemble d'alertes complètes satisfaisant la requête afin de permettre le raffinement de cette requête.

Une requête de l'opérateur de sécurité est une formule logique f, qui combine des conjugaisons $\wedge$, des disjonctions $\vee$, et des négations $\neg$ d'attributs valués.

D'une manière générale, la description $d(o)$ d'une alerte o satisfait une requête f, si la requête f est une conséquence logique de la description $d(o)$. L'ensemble des alertes satisfaisant la requête f, appelé l'extension de f, est ainsi donné par $ext(f) = \{o \in \mathcal{O} : d(o) \models f\}$.

L'ensemble A des attributs valués pertinents est l'ensemble des attributs valués appartenant à des domaines d'attributs valués $\mathcal{A}$, tel que pour tout attribut valué pertinent p de $\mathcal{A}$, l'ensemble d'alertes complètes satisfaisant la conjonction de la requête courante f avec l'attribut valué pertinent p est contenu strictement dans l'ensemble d'alertes complètes satisfaisant la requête courante f. Ainsi, cet ensemble A des attributs valués pertinents qui permettent de distinguer des alertes entre elles, peut être défini de la façon suivante :

$$A = \{p \in \mathcal{A} : \phi \subset ext(f \wedge p) \subset ext(f)\}.$$

L'ensemble $\mathcal{A}$ peut être considéré comme un ensemble des liens de navigation, en définissant chaque attribut valué pertinent p comme un lien de navigation. L'opérateur de sécurité peut ainsi raffiner sa requête courante f en choisissant un lien de navigation $p \in A$ fourni par le système de gestion d'alertes 13. La requête courante f de l'opérateur de sécurité se transforme ainsi en la nouvelle requête $f \wedge p$.

Avantageusement, pour réduire encore plus le nombre de réponses, le système de gestion d'alertes 13 fournit, en priorité, les attributs valués pertinents les plus généraux en regard de la pluralité de structures taxinomiques.

L'ensemble $A_{\max}$ des attributs valués pertinents les plus généraux est alors donné par l'ensemble $\max_{|=}(A)$ qui peut être défini de la façon suivante :

$$\max_{|=}(A) = \{ p \in A \text{ : } \textit{il n'existe pas } p' \in A, p' \neq p, p \mid= p' \}.$$

Ainsi, cet ensemble $\max_{|=}(A)$, est l'ensemble de tout attribut valué pertinent p de A qui n'a pas un attribut valué plus général.

En outre, en réponse à la requête courante f, le système de gestion d'alertes fournit un ensemble O d'identifiants d'alertes dont la description satisfait la requête courante f et ne pouvant pas être raffinée, c'est-à-dire décrite plus précisément, par rapport à cette requête f. Ainsi, l'ensemble O des identifiants d'alertes comporte tout identifiant d'alerte dont la description satisfait la requête courante f et telle qu'il n'existe aucun attribut valué pertinent p tel que la conjonction de f et de p soit satisfaite par la description de cette même alerte. Ainsi, cet ensemble O peut être défini de la façon suivante :

$O = \{ id(o) : o \in \mathcal{O},\ d(o) \mid= f$, et il n'existe pas $p \in A$ avec $d(o) \mid= f \wedge p \}$.

On notera que le système de fichiers logique 21 tel que LISFS offre des commandes permettant de naviguer (commande « cd »), interroger (commande « ls »), et stocker (commandes « cp » et mkdir ») des objets.

Par exemple, dans LISFS, une requête permettant d'obtenir les alertes dont la victime est un *proxy web* et dont l'attaquant n'est pas interne s'exprime de la façon suivante :

ls / "victime web proxy"/! "attaquant interne".

D'une manière générale, une alerte provenant d'une sonde de détection d'intrusions est un quadruplet d'attributs valués. Les quatre attributs envisagés sont : *attaque, attaquant, victime, et date*.

Le domaine de l'attribut valué « *attaque* » est constitué des identifiants de signatures d'attaques contenus dans les alertes générées par les sondes de détection d'intrusions 11a, 11b, 11c.

Le domaine de l'attribut valué d'attaque comporte aussi les vulnérabilités éventuellement exploitées par une attaque. Les vulnérabilités sont plus abstraites, c'est-à-dire plus générales, que les identifiants d'attaques.

Les autres valeurs utilisées pour qualifier les attaques sont issues des mots clés employés pour qualifier les attaques dans une documentation des sondes de détection d'intrusions 11a, 11b, 11c.

A titre d'exemple, on peut utiliser la sonde Snort™ et le champ « *msg* » de la documentation des signatures.

En effet, la figure 3A illustre un exemple de documentation associée aux signatures d'attaques.

La colonne 31 du tableau 33 comporte des nombres entiers désignant les signatures d'attaques. La colonne 35 du tableau 33 comporte les documentations associées à ces signatures d'attaques. Ainsi, dans chaque ligne du tableau 33, une documentation est associée à chaque signature d'attaque. Chaque description comporte des mots clés relatifs par exemple au type d'attaque, au protocole réseau utilisé, et au succès ou à l'échec de l'attaque.

La figure 3B montre une structure taxinomique 37 définissant des relations de généralisation 39 entre les attributs valués contenus dans le tableau 33. Cette structure taxinomique 37 est organisée selon des connaissances expertes, à partir des mots clés de la documentation des signatures du tableau 33. On notera que, les signatures d'attaques 31 constituent les attributs valués les plus spécifiques.

Le domaine de l'attribut valué « attaquants » comporte des adresses IP. Les adresses IP externes sont généralisables par le nom de l'organisme propriétaire de la plage d'adresses IP à laquelle appartient

l'adresse. Le nom de l'organisme correspond au champ « *netname* » contenu dans des bases de données de l'organisme IANA™, qui gère l'attribution d'adresses IP.

Les adresses IP internes et les adresses IP privées (non routables), sont généralisables en identifiants de réseaux locaux définis par un administrateur du système de détection d'intrusions 1.

Enfin les noms des organismes sont généralisables en la valeur « *ext* » et les identifiants des réseaux locaux sont généralisables en la valeur « *int* ».

Le domaine de l'attribut valué « *victime* » comporte des adresses IP. Ces adresses IP des victimes peuvent être généralisées en l'adresse du réseau local correspondant.

Ces adresses IP peuvent aussi être généralisées en noms de machines, obtenus par des mécanismes de résolution de noms. Les noms de machines peuvent être généralisés en « *fonctions* » d'hôtes (par exemple serveur web), définis par l'administrateur du site. Les noms de machines sont généralisables en identifiants de réseaux locaux définis par l'administrateur du réseau (par exemple DMZ).

Le domaine de l'attribut valué « date » comporte l'horodatage des alertes au format JJ-MM-AAAA hh:mm:ss. Les dates sont généralisées successivement en minutes, heure, jour, et mois dans l'année. Ces généralisations correspondent finalement à des abstractions de plus en plus grossières de la date d'une attaque.

Revendications

1.Procédé de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions (11a, 11b, 11c) d'un système de sécurité d'informations (1) comportant un système de gestion d'alertes (13), chaque alerte étant définie par un identifiant d'alerte et un contenu d'alerte, caractérisé en ce qu'il comporte les étapes suivantes :

-associer à chacune des alertes issues des sondes de détection d'intrusions (11a, 11b, 11c), une description comportant une conjonction d'une pluralité d'attributs valués appartenant à une pluralité de domaines d'attributs ;

-organiser les attributs valués appartenant à chaque domaine d'attributs en une structure taxinomique définissant des relations de généralisation entre lesdits attributs valués, la pluralité des domaines d'attributs formant ainsi une pluralité de structures taxinomiques ;

-compléter la description de chacune desdites alertes par des ensembles de valeurs induites par les structures taxinomiques à partir des attributs valués desdites alertes pour former des alertes complètes ;

-stocker lesdites alertes complètes dans un système de fichiers logique (21) pour en permettre la consultation.

2.Procédé selon la revendication 1, caractérisé en ce que la consultation des alertes complètes est réalisée par une succession d'interrogations et/ou de navigations dans lesdites alertes complètes de sorte qu'en réponse à une requête, le système de gestion d'alertes (13) fournit des attributs valués pertinents permettant de distinguer un sous-ensemble d'alertes complètes parmi un ensemble d'alertes complètes satisfaisant la requête afin de permettre le raffinement de ladite requête.

3.Procédé selon la revendication 2, caractérisé en ce que les attributs valués pertinents sont en priorité les plus généraux au regard de la pluralité de structures taxinomiques.

4.Procédé selon l'une quelconque des revendications 2 et 3, caractérisé en ce qu'en réponse à la requête, le système de gestion d'alertes (13) fournit en outre des identifiants d'alertes satisfaisant la requête et dont la description ne peut pas être raffinée par rapport à ladite requête.

5.Procédé selon la revendication 1, caractérisé en ce que l'identifiant d'alerte est un couple formé d'un identifiant de la sonde de détection d'intrusions (11a, 11b, 11c) qui produit l'alerte et d'un numéro de série d'alerte affecté par ladite sonde.

6.Procédé selon la revendication 1, caractérisé en ce que le contenu de chaque alerte comporte un message textuel fourni par la sonde de détection d'intrusions (11a, 11b, 11c) correspondante.

7.Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que chaque attribut valué comporte un identifiant d'attribut et une valeur d'attribut.

8.Procédé selon la revendication 7, caractérisé en ce que chaque identifiant d'attribut est associé à un domaine d'attributs parmi les domaines suivants : domaine de l'attaque, domaine de l'identité de l'attaquant, domaine de l'identité de la victime et domaine de la date de l'attaque.

9.Procédé selon la revendication 1, caractérisé en ce que la description d'une alerte donnée est complétée en récupérant à partir des relations de

généralisation de la pluralité de structures taxinomiques et de manière récursive, un ensemble comportant les attributs valués plus généraux et n'ayant pas déjà été présents dans la description d'une autre alerte précédemment complétée.

10.Procédé selon l'une quelconque des revendications 1 à 9, caractérisé en ce que les attributs valués dans la structure taxinomique sont organisés selon un graphe acyclique dirigé.

11. Programme informatique caractérisé en ce qu'il est conçu pour mettre en œuvre le procédé selon l'une quelconque des revendications 1 à 10 lorsqu'il est exécuté par le système de gestion d'alertes (13).

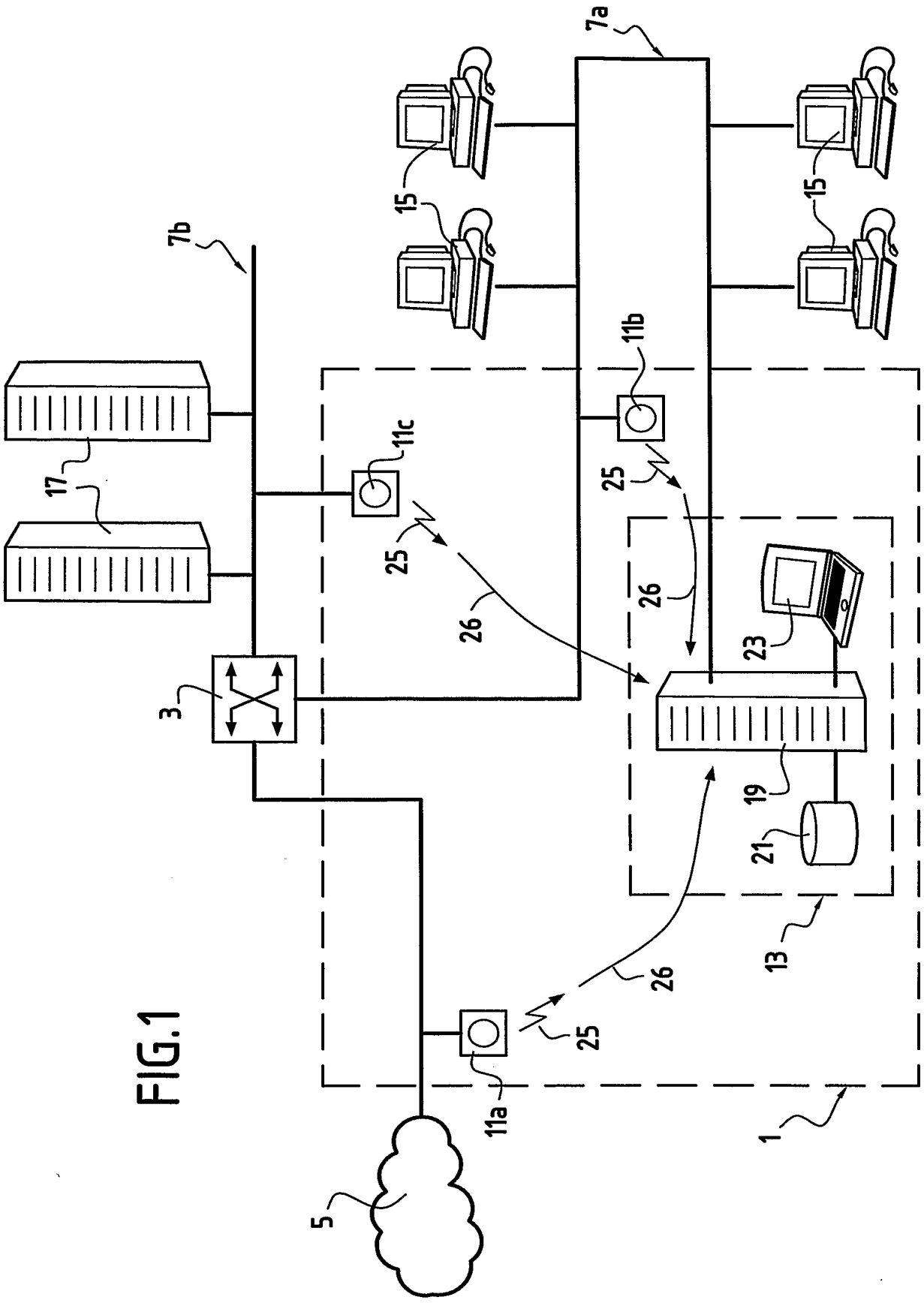


FIG.1

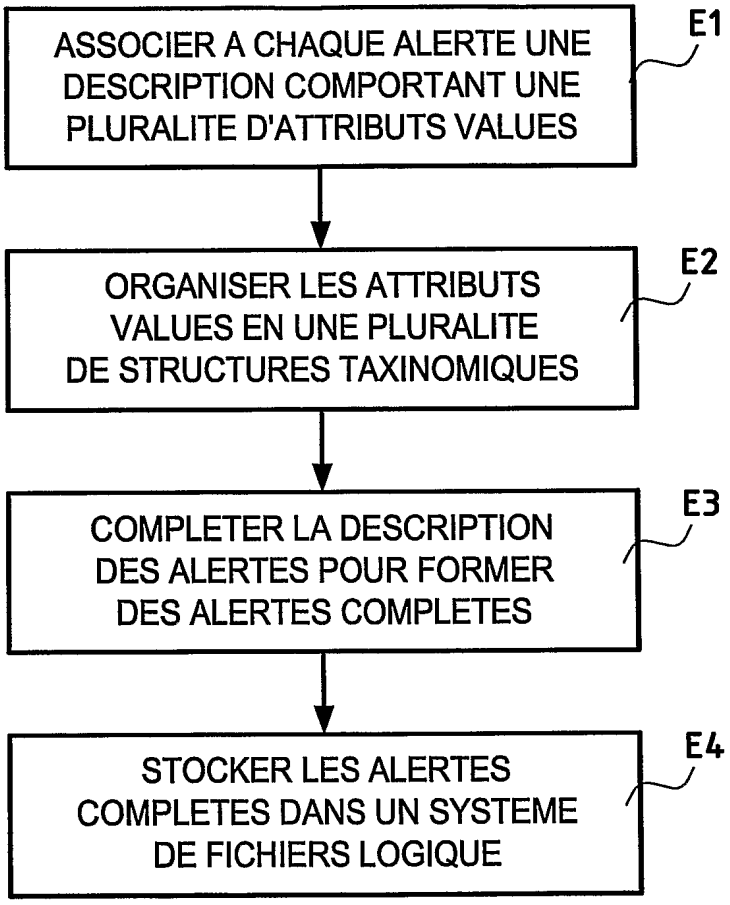

ASSOCIER A CHAQUE ALERTE UNE DESCRIPTION COMPORTANT UNE PLURALITE D'ATTRIBUTS VALUES
E1
ORGANISER LES ATTRIBUTS VALUES EN UNE PLURALITE DE STRUCTURES TAXINOMIQUES
E2
COMPLETER LA DESCRIPTION DES ALERTES POUR FORMER DES ALERTES COMPLETES
E3
STOCKER LES ALERTES COMPLETES DANS UN SYSTEME DE FICHIERS LOGIQUE
E4

FIG.2

31 35

Sig. Id	Documentation
1739	WEB-PHP DNSTools administror authentication bypass attempt (tentative de contournement de l'authentification de l'administrateur)
1740	WEB-PHP DNSTools authentication bypass attempt (tentative de contournement de l'authentification)
1741	WEB-PHP DNSTools access (accès)
803	WEB-CGI HyperSeek hsx.cgi directory traversal attempt (tentative de remontée de répertoire)
1076	WEB-IIS repost.asp access (accès)
1110	WEB-MISC apache source.asp file access (accès au fichier)
340	FTP EXPLOIT overflow (débordement de zone mémoire)
1247	WEB-FRONTPAGE rad overflow attempt (tentative de débordement de zone mémoire)

33

FIG.3A

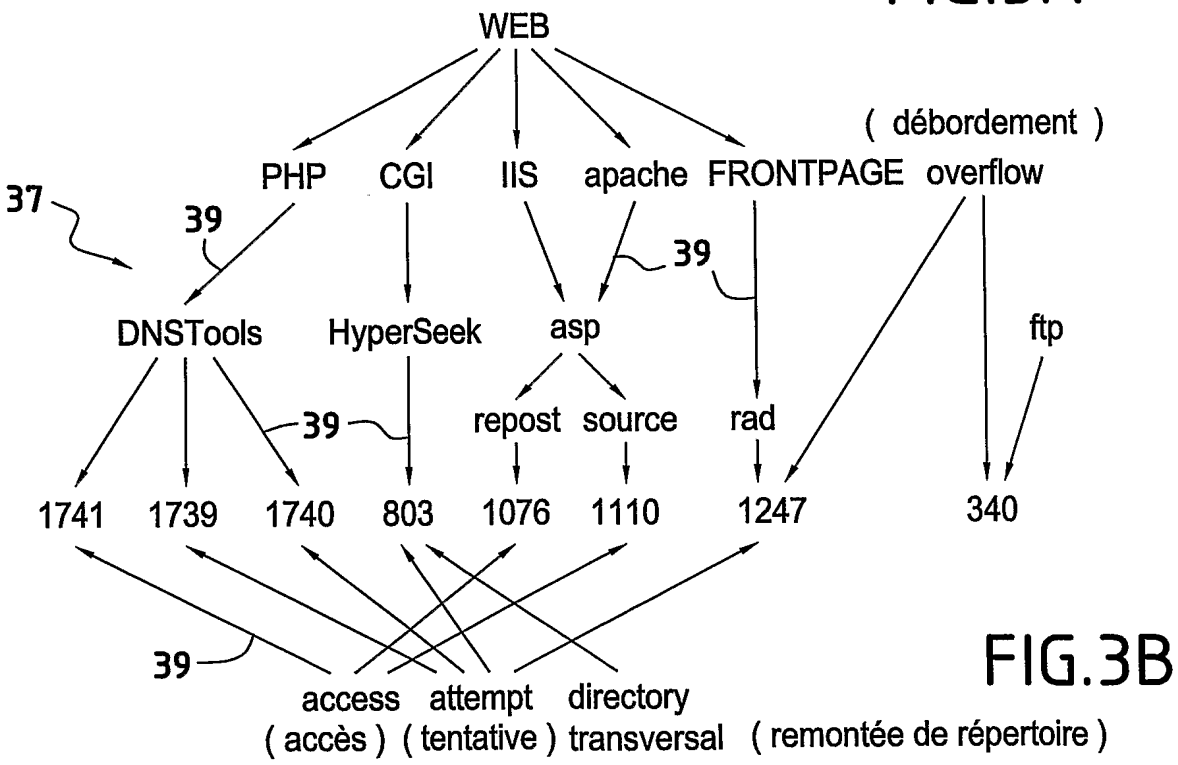


FIG.3B

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/003252

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F17/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	YOANN PADIOLEAU AND OLIVIER RIDOUX: "A Logic File System" PROCEEDINGS OF THE 2003 USENIX ANNUAL TECHNICAL CONFERENCE, 'Online! 9 June 2003 (2003-06-09), - 14 June 2003 (2003-06-14) XP002291663 SAN ANTONIO, TEXAS, USA Retrieved from the Internet: URL:http://www.usenix.org/events/usenix03/tech/full_papers/padioleau/padioleau.pdf> 'retrieved on 2004-08-09! the whole document ----- -/--	1-11

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 May 2005	24/05/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bertolissi, E

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/003252

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DEBAR H ET AL: "A REVISED TAXONOMY FOR INTRUSION-DETECTION SYSTEMS" ANNALES DES TELECOMMUNICATIONS - ANNALS OF TELECOMMUNICATIONS, PRESSES POLYTECHNIQUES ET UNIVERSITAIRES ROMANDES, LAUSANNE, CH, vol. 55, no. 7/8, July 2000 (2000-07), pages 361-378, XP000954771 ISSN: 0003-4347 abstract	1-11
A	ULF LINDQVIST AND ERLAND JONSSON: "How to Systematically Classify Computer Security Intrusions" PROCEEDINGS OF THE 21ST NATIONAL INFORMATION SYSTEMST SECURITY CONFERENCE, 'Online! 4 May 1997 (1997-05-04), - 8 May 2003 (2003-05-08) pages 154-163, XP002291664 OAKLAND, CALIFORNIA Retrieved from the Internet: URL:http://www.ce.chalmers.se/old/staff/ulf1/pubs/sp97ul.pdf> 'retrieved on 2004-08-09! abstract	1-11
A	EP 1 146 689 A (MITEL KNOWLEDGE CORP) 17 October 2001 (2001-10-17) abstract paragraph '0011! - paragraph '0017!; figures 2-4	1-11
A	EP 0 735 477 A (ALCATEL ITALIA ; ALCATEL NV (NL)) 2 October 1996 (1996-10-02) abstract column 3, line 15 - column 5, line 5; figures 2,4	1-11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR2004/003252

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1146689 A	17-10-2001	GB 2361382 A	17-10-2001
		CA 2343695 A1	12-10-2001
		EP 1146689 A2	17-10-2001
		US 2002021788 A1	21-02-2002
EP 0735477 A	02-10-1996	IT MI950646 A1	30-09-1996
		AU 711489 B2	14-10-1999
		AU 4806296 A	10-10-1996
		EP 0735477 A1	02-10-1996

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR2004/003252

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L29/06 G06F17/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	YOANN PADIOLEAU AND OLIVIER RIDOUX: "A Logic File System" PROCEEDINGS OF THE 2003 USENIX ANNUAL TECHNICAL CONFERENCE, 'Online! 9 juin 2003 (2003-06-09), - 14 juin 2003 (2003-06-14) XP002291663 SAN ANTONIO, TEXAS, USA Extrait de l'Internet: URL:http://www.usenix.org/events/usenix03/tech/full_papers/padioleau/padioleau.pdf> 'extrait le 2004-08-09! le document en entier -/--	1-11

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
10 mai 2005	24/05/2005

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bertolissi, E

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR2004/003252

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	DEBAR H ET AL: "A REVISED TAXONOMY FOR INTRUSION-DETECTION SYSTEMS" ANNALES DES TELECOMMUNICATIONS - ANNALS OF TELECOMMUNICATIONS, PRESSES POLYTECHNIQUES ET UNIVERSITAIRES ROMANDES, LAUSANNE, CH, vol. 55, no. 7/8, juillet 2000 (2000-07), pages 361-378, XP000954771 ISSN: 0003-4347 abrégé	1-11
A	ULF LINDQVIST AND ERLAND JONSSON: "How to Systematically Classify Computer Security Intrusions" PROCEEDINGS OF THE 21ST NATIONAL INFORMATION SYSTEMST SECURITY CONFERENCE, 'Online! 4 mai 1997 (1997-05-04), - 8 mai 2003 (2003-05-08) pages 154-163, XP002291664 OAKLAND, CALIFORNIA Extrait de l'Internet: URL:http://www.ce.chalmers.se/old/staff/ulfl/pubs/sp97ul.pdf> 'extrait le 2004-08-09! abrégé	1-11
A	EP 1 146 689 A (MITEL KNOWLEDGE CORP) 17 octobre 2001 (2001-10-17) abrégé alinéa '0011! - alinéa '0017!; figures 2-4	1-11
A	EP 0 735 477 A (ALCATEL ITALIA ; ALCATEL NV (NL)) 2 octobre 1996 (1996-10-02) abrégé colonne 3, ligne 15 - colonne 5, ligne 5; figures 2,4	1-11

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR2004/003252

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 1146689	A	17-10-2001	GB	2361382 A	17-10-2001
			CA	2343695 A1	12-10-2001
			EP	1146689 A2	17-10-2001
			US	2002021788 A1	21-02-2002
EP 0735477	A	02-10-1996	IT	MI950646 A1	30-09-1996
			AU	711489 B2	14-10-1999
			AU	4806296 A	10-10-1996
			EP	0735477 A1	02-10-1996